

GLOSSARY OF OPSEC TERMS

A

Acceptable Level of Risk: An authority's determination of the level of potential harm to an operation, program, or activity due to the loss of information that the authority is willing to accept.

Accepted Risk: The acknowledgment that a protection system may not achieve 100 percent protection against all occurrences, but further improvement in the system is not justified, and that the Department is willing to accept the potential consequences of an adversarial act.

Access Control: The process of permitting access or denying access to information, facilities, nuclear materials, resources, or designated security areas.

Access Control Mechanisms: Measures or procedures designed to prevent unauthorized access to protected information or facilities.

ACINT: See Acoustic Intelligence.

Acoustic Intelligence: Intelligence information derived from the collection and analysis of acoustical phenomena.

Adversary: Any government, organization, group, or individual whose interests are adverse to those of the U.S. Government in general and to those of the Department in particular that must be denied critical information. Synonymous with competitor/enemy.

Adversary Collection Methodology: Any resource and method available to and used by an adversary for the collection and exploitation of sensitive/critical information or indicators thereof.

Adversary Threat Strategy: The process of defining, in narrative or graphical format, the threat presented to an operation, program, or project. The adversary threat strategy should define the potential adversaries, the courses of action those adversaries might take against the operation, and the information needed by the adversaries to execute those actions.

Agent: A person who engages in a clandestine activity.

AIS: See Automated Information Systems.

Analysis: The process by which information is examined in order to identify significant facts and/or derive conclusions.

Assessment: To evaluate the worth, significance, or status of something; especially to give an expert judgment of the value or merit of something.

Asset: 1. Any resource—a person, group, relationship, instrument installation, supply—at the disposition of an intelligence agency for use in an operational or support role. 2. A person who contributes to a clandestine mission but is not a fully controlled agent.

Authentication: Security measures designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Authenticity: Having an undisputed identity or origin.

Automated Information Systems: An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Availability: The assurance that data transmissions, computer processing systems, and/or communications are not denied to those who are authorized to use them.

B No Definition

C

Camouflage: The use of natural or artificial material on personnel, objects, or positions (e.g., tactical) in order to confuse, mislead, or evade the enemy/adversary.

Case Officer: A professional employee of an intelligence organization who is responsible for providing direction for an agent operation. CCD. See the individual components: camouflage; concealment; and deception.

Clandestine Operation: 1. An operation sponsored or conducted by government departments or agencies in such a way as to insure secrecy or concealment. 2. An operation sponsored or conducted in such a way as to insure the secrecy or concealment of the person or organization doing the sponsoring/conducting. See also covert operation; overt operation.

Classification: The determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made; the designation is normally termed a security classification and includes Confidential, Secret, and Top Secret.

Classification Guide: A documentary form of classification guidance, issued by an original classification authority. It identifies the elements of information, regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Classified Information: Information that has been determined, pursuant to Executive Order 12598 or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

COMINT: See Communications Intelligence.

Command and Control Warfare: The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction. **C2W** is mutually supported by intelligence to deny information to, influence, degrade, or destroy adversary command and control capabilities. This process is accomplished while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict.

C2W: See Command and Control Warfare.

Commercial-Off-The-Shelf: Any commercially available hardware or software. Communications deception. Deliberate transmission, retransmission, or alteration of communications in order to mislead an adversary's interpretation of the communications.

Communications Intelligence: Technical and intelligence information derived from the intercept of foreign communications by other than the intended recipients of those communications.

Communications Profile: An analytic model of communications associated with an organization or activity. The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the COMSEC measures applied.

Communications Security: Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

Compartmentation: 1. A formal system for restricting access to selected activities or information. 2. The establishment and management of an organization so that information about the personnel, internal organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties.

Competitor: See adversary.

Compromise: Unauthorized intentional or unintentional disclosure of information or data to unauthorized persons. Compromise is also a security policy violation of a system in which, modification, destruction, or loss of an object may have occurred.

Compromising Emanations: Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information systems equipment. NOTE: This is also known as TEMPEST.

COMPUSEC: See Computer Security.

Computer Security: Measures and controls that ensure confidentiality, integrity, and availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated.

COMSEC: See Communications Security.

COMSEC Monitoring: The act of listening to, copying, or recording transmissions of one's own official telecommunications in order to analyze the degree of security.

Concealment: The act of remaining hidden.

Confidential Source: Any individual or organization that provides information to the United States government on matters pertaining to the national security and expects, in return, that the information or relationship, or both, will be held in confidence.

Confidentiality: An assurance that information is not disclosed to unauthorized entities or processes.

Contingency Plan: Plan maintained for emergency response, backup operations, and post-disaster recovery for an information system, to ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Controlled Information: Information and indicators deliberately conveyed or denied to foreign targets in order to evoke invalid official estimates that result in foreign official actions advantageous to U.S. interests and objectives.

COTS: See commercial-off-the-shelf

Counterintelligence: 1. That phase of intelligence covering all activity designed to neutralize the effectiveness of adversary intelligence collection activities. 2. Those activities that are concerned with identifying and counteracting the security threat posed by hostile intelligence services, organizations, or by individuals engaged in espionage, sabotage, subversion, or terrorism.

Countermeasure: Anything which effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

Cover: Protective action taken to mask or conceal an operation or activity from an adversary.

Covert Operation: An operation that is so planned and executed as to conceal the identity of, or permit plausible denial by, the sponsor. A covert operation differs from a clandestine operation

in that emphasis is placed on concealment of the identity of the sponsor, rather than on concealment of the operation. Synonymous with law enforcement's undercover operation.

CPI: See Critical Program Information.

Critical Information: Specific facts about friendly (e.g., U.S.) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives.

Critical Infrastructures: Certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

Critical Program Information: Information concerning sensitive activities, whether classified or unclassified, that is vitally needed by adversaries or competitors for them to plan and act effectively. NOTE: Formerly, that information on what was called the “critical and sensitive information list”. (Operations Security)

Cryptanalysis: Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

Crypto-equipment: The equipment used to render plain information unintelligible and restore encrypted information to intelligible form.

Cryptography: Art or science concerning the principles means, and methods for rendering plain information unintelligible and of restoring encrypted information to intelligible form.

Cryptosecurity: A component of communications security resulting from the provisions of technically sound cryptosystems and their proper use.

Cyber Security: The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, against loss of accountability for information and user actions, and against the denial of service to authorized users, including those measures necessary to protect against, detect, and counter such threats.

D

Damage: A loss of friendly effectiveness due to adversary action. Synonymous with harm.

Deception: Those measures designed to mislead the enemy/adversary by manipulation, distortion, or falsification of evidence in order to induce a reaction from that adversary which is prejudicial to the adversary's interests.

Defense Information Infrastructure: The DII encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the DOD's local and worldwide information needs. The DII (a) connects DOD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and (b) provides information processing and value-added services to subscribers over the DISN. Unique user data, information, and user applications are not considered part of the DII.

Defense Information Systems Network: 1. A sub-element of the DII, the DISN is the DOD's consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. 2. The DISN is an information transfer network with value-added services for supporting national defense C3I decision support requirements and CIM functional business areas. As a[n] information transfer utility, the DISN provides dedicated point-to-point, switched voice and data, imagery and video teleconferencing communications services.

Denial: 1. The act of disowning or disavowing. 2. The refusal to grant something. See also deception; denial of service.

Denial of Service: When action(s) result in the inability to communicate and/or the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of a signal or operational capability detectable actions. Physical actions or whatever can be heard, observed, imaged, or detected by human senses, or by active and/or passive technical sensors, including emissions that can be intercepted.

Design Basis Threat (DBT): The statement that describes threats that are postulated for the purpose of analyzing S&S programs, systems, components, equipment, information, or material [see DOE O 470.3, *Design Basis Threat Policy (U)*].

DF: See Direction Finding.

DII: See Defense Information Infrastructure.

Direction Finding: A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment disclosure. The release of information through approved channels.

DISN: See Defense Information Systems Network.

E

Economic Intelligence: Intelligence regarding economic resources, activities, and policies.

Electronic Intelligence: Technical and geolocation intelligence derived from foreign non-communications transmissions (e.g., radar) by other than nuclear detonations or radioactive sources.

Electronic Security: Protection resulting from measures designed to deny unauthorized persons information from the interception and analysis of noncommunication electromagnetic emissions, such as radar.

Electronic Warfare: Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support.

ELINT: See Electronic Intelligence.

ELSEC: See Electronic Security.

Emissions Security: Protection resulting from measures taken to deny unauthorized persons information derived from the intercept and analysis of compromising emanations from crypto-equipment or an information system.

EMSEC: See Emission Security.

Enemy: See adversary.

Espionage: 1. The act or practice of spying or of using spies to obtain secret intelligence. 2. Overt, covert, or clandestine activity. A term which is usually used in conjunction with the country against which such an activity takes place. For example, espionage against the U.S.

EW: See Electronic Warfare.

Exploitation: The process of obtaining intelligence information from any source and taking advantage of it.

F

Facilities: Buildings, structures, or other real property. Entities such as military bases, industrial sites, and office complexes may be identified as facilities.

Firewall: A system designed to prevent unauthorized access to or from a private network.

Foe: An opponent; the antithesis of friend.

FOIA: See Freedom of Information Act.

Foreign Intelligence Service: An organization of a foreign government that engages in intelligence activities.

Foreign National: Any person who is not a U.S. citizen (i.e., not a U.S. national); any corporation not incorporated in the U.S.; any international organization; foreign government; or any agency or subdivision of foreign government (e.g., diplomatic missions). (Security)

Freedom of Information Act: A provision that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

Friend: A country, individual, or organization with whom one is allied in a struggle or cause.

Friendly: An adjective that describes an operation or activity that is carried out by a friend (e.g., friendly fire).

G

GIL: See Global Information Infrastructure.

Global Information Infrastructure: The information systems of all countries, international and multinational organizations, and multi-international commercial communications services.

GOTS: See government-off-the-shelf.

Government-Off-The-Shelf: An item that has been developed by the government and produced to military or commercial standards and specifications, is readily available for delivery from an industrial source, and may be procured without change to satisfy a military requirement.

H

Hacker: An individual who gains unauthorized access to an automated information system.

Human Intelligence: A category of intelligence derived from information collected and/or provided by human sources.

HUMINT: See Human Intelligence.

I

IA: See Information Assurance.

1C: See Intelligence Community.

Identification: See authentication.

Imagery: Collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media.

Imagery Intelligence: Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media.

IMINT: See Imagery Intelligence.

Imitative Communications Deception: Introduction of deceptive messages or signals into an adversary's telecommunications signals.

Inadvertent Disclosure: Accidental exposure of information to a person not authorized access.

Incident: An assessed event of attempted entry, unauthorized entry, and/or attack against a facility, operation, or an AIS.

Indicators: Sources of information that, if exploited by an adversary or competitor, could reveal critical program information. An indicator can be identified by asking the question, "If I were an adversary or competitor, where would I go to obtain critical program information?" NOTE: Formerly called "essential elements of friendly information". (Operations Security)

Industrial Espionage: The act of seeking a competitive, commercial advantage by obtaining a competitor's trade secrets and/or logistics. The acquisition of industrial information through clandestine operations.

Information: Any knowledge that can be communicated and/or any documentary material regardless of its physical form or characteristics.

Information Assurance: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Integrity: The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed. See also integrity.

Information Operation: Any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces.

Information Security: The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

Information Systems Security: The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Information Warfare: 1. Actions taken to achieve information superiority by adversely affecting an adversary's information, information-based processes, and/or information systems while defending one's own information, information-based processes, and/or information systems (DOD JP 1994). 2. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

INFOSEC: See Information Systems Security.

INFOWAR: See Information Warfare.

Integrity: Absolute verification that data or information has not been modified in transmission or during computer processing. See also information integrity.

Intelligence: Information and/or knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

Intelligence Collection: The act of gathering information from all available sources to meet an intelligence requirement.

Intelligence Community: The aggregate of the following executive branch organizations and agencies involved in intelligence activities: the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; intelligence elements of the military services, the Federal Bureau of Investigation, the Department of the Treasury, and the Department of Energy; and staff elements of the Office of the Director of Central Intelligence.

Intelligence Cycle: The steps by which information is converted into intelligence and made available to users. The cycle has been described as including five steps: planning and direction; collection; processing; production; and dissemination.

Intelligence Data: See intelligence information.

Intelligence Information: Unevaluated material that may be used in the production of intelligence.

Information of Intelligence Value: Synonymous with intelligence data.

Intelligence System: Any system (formal or informal) which is used to manage data gathering, obtain and process the data, interpret the data, and provide analytically-sound opinions to decision makers in order that they may make informed decisions with regard to various courses of action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks.

Intention: An aim or design (as distinct from a capability) to execute a specified course of action.

Intercept: 1. Data which is obtained through the passive collection of signals. Interrupting access, communication, or the flow of a process.

10: See Information Operation.

Insider: A person who, by reason of official duties, has knowledge of operations and/or security system characteristics, and/or position that would significantly enhance the likelihood of successful bypass or defeat of positive measures should that person attempt such an action.

IW: See Information Warfare.

J No Definition

K No Definition

L

Local Threat Assessment: A threat assessment for a specific facility or operation.

Low Probability of Detection: The result of measures used to hide or disguise intentional electromagnetic transmissions.

Low Probability of Intercept: Result of measures to prevent the intercept of intentional electromagnetic transmissions.

LPD: See Low Probability of Detection.

LPL: See Low Probability of Intercept.

M

Manipulative Communications Deception: Alteration or simulation of friendly telecommunications for the purpose of deception.

MASINT: See Measurement and Signature Intelligence.

Measurement and Signature Intelligence: Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic). This data is derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender. This facilitates subsequent identification and or measurement of the same.

MLS: See Multilevel Security.

Multilevel Security: The concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.

N

National Information Infrastructure: 1. The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It includes both public and private networks, the Internet, the public switched network, and cable, wireless, and satellite communications.

National Security: Measures adopted by the government of a nation in order to assure the safety of its citizens, guard against attack, and prevent disclosure of sensitive or classified information which might threaten or embarrass said nation.

Need-to-Know: A determination which is made by an authorized holder of classified or proprietary information as to whether or not a prospective recipient requires access to specific the information in order to perform or assist in a lawful and authorized governmental function.

NIL: See National Information Infrastructure.

Nonrepudiation: Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data. Digital signatures are the current non-repudiation technique of choice for the Nil.

O

Observables: Any actions that reveal indicators which are exploitable by adversaries.

Open Source Intelligence: Information of potential intelligence value that is available to the general public.

Operations Security: 1. A systematic, proven process by which a government, organization, or individual can identify, control, and protect generally unclassified information about an operation/activity and, thus, deny or mitigate an adversary's/competitor's ability to compromise or interrupt said operation/activity. 2. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to (a) identify those actions that can be observed by adversary intelligence systems, (b) determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Operations Security Assessment: A thorough evaluation of the effectiveness of a customer's implementation of OPSEC methodology, resources, and tools. Assessments (a) are used to evaluate the effectiveness of the customer's corporate level OPSEC program and (b) can be used at the program level to determine whether or not a program is a viable candidate for an OPSEC survey.

Operations Security Plan: A strategy that analyzes an operation or activity and includes specific operations security measures.

Operations Security Process: An analytical process that involves five components: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Operations Security Program: An OPSEC program is the vehicle by which the principles and practices of OPSEC are employed within an organization.

Operations Security Survey: The application of OPSEC methodology at the program level. It is a detailed analysis of all activities associated with a specific operation, project or program in order to determine what exploitable evidence of classified or sensitive activity could be acquired in light of the known collection capabilities of potential adversaries.

Operations Security working group A (normally formally) designated body representing a broad range of line and staff activities within an organization that provides OPSEC advice and support to leadership and all elements of the organization.

OPSEC: See Operations Security.

OSINT: See Open Source Intelligence.

Overt collection: The acquisition of information via the public domain.

Overt operation An operation conducted openly, without concealment.

P

Perceived Collection Threat: An estimate of the present and future resource allocations and capabilities of an adversary to gain information. Synonymous with potential threat.

Physical Security: 1. The application of physical barriers and control procedures as countermeasures against threats to resources and sensitive information. 2. The security discipline concerned with physical measures designed to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Potential Threat: See perceived collection threat.

Procurement: The process of obtaining personnel, services, supplies, and equipment.

Profile: A collection and/or display (e.g., a written or graphical description) of the signatures and patterns of an individual or organization.

Proprietary Information: Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that have been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the government or to the public without restriction from another source.

Protected Information: Includes sensitive, critical and/or classified information.

Protective Measures: Those actions, procedures, or designs implemented to safeguard protected information.

Psychological Operations: Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and, ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

PSYOP: See Psychological Operations.

Public Domain: In open view; before the public at large and not in private or employing secrecy or other protective measures.

Q No Definition

R

Red/Black Concept: The separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information, in electrical signal form, from those which handle unclassified (BLACK) information in the same form.

Residual Risk: The portion of risk remaining after security measures (countermeasures) have been applied.

Risk: A measure of the potential degree to which protected information is subject to loss through adversary exploitation.

Risk Analysis: A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios in order to determine the likelihood of compromise of critical information.

Risk Assessment: An OPSEC process of evaluating the risks of information loss based on an analysis of threats to, and vulnerabilities of, a system, operation, or activity.

Risk Avoidance: A security philosophy which postulates that adversaries are all-knowing and highly competent, against which risks are avoided by maximizing defenses and minimizing vulnerabilities.

Risk Management: A security philosophy which considers actual threats, inherent vulnerabilities, and the availability and costs of countermeasures as the underlying basis for making security decisions.

S

SAP: See Special Access Program.

Security: Precautions taken to establish and maintain an acceptable level of protection.

Secure Communications: Telecommunications deriving security through use of type 1 products and/or protected distribution systems.

Sensitive Information: Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

SIGINT: See Signals Intelligence.

Signals Intelligence: A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted.

Signals Security: Generic term encompassing communications security and electronic security.

SIGSEC: See Signals Security.

Special Access Program: A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Surveillance: The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, photographic, or other means.

T

TAISS: See Telecommunications and Automated Information Systems Security.

Target: An individual, operation, or activity which an adversary has determined possesses information that might prove useful in attaining his/her objective.

Technical Security: The programs established primarily to protect classified and unclassified controlled information, such as technical surveillance countermeasures, communications security, emission security, and TEMPEST.

Technical Surveillance: The covert devices, equipment, techniques, and measures used to obtain unauthorized access to classified and/or unclassified controlled information.

Technical Surveillance Countermeasures (TSCM). The techniques and measures used to detect and nullify the technologies that are intended to obtain unauthorized access to classified and/or unclassified controlled information.

Telecommunications: Preparation, transmission, communication or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

Telecommunications and Automated Information Systems Security: Superseded by Information Systems Security.

Telemetry: The science and technology of automatic data measurement and transmission, as by wire or radio, from remote sources, such as space vehicles, to a receiving station for recording and analysis.

Telemetry Intelligence: Technical and intelligence information derived from intercept, processing, and analysis of foreign telemetry; a subcategory of foreign instrumentation signals intelligence.

TELINT: See Telemetry Intelligence.

TEMPEST: Short name referring to investigation, study, and control of compromising emanations from telecommunications and information systems equipment.

Terrorism: The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Trash Collector Intelligence: TRASHINT or Dumpster Diving is the colloquial name for going through someone's garbage/trash/recycled paper. It is also a great tactic for gaining information about an organization, person, company, and research and development in progress. Trash handling involves two basic categories, general trash, and paper waste.

TRASHINT: See Trash Collector Intelligence.

Threat: The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operations.

Threat Analysis: An OPSEC process, which examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.

Threat Assessment: An evaluation of the intelligence collection threat to a program activity, system, or operation.

Threat Information: Unevaluated material of every description, at all levels of reliability, and from any source that may contain knowledge or intelligence about a threat.

Trade Secret: See proprietary information.

TRANSEC See Transmission Security.

Transmission Security: Component of communications security from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

Type 1 Products: Classified or controlled cryptographic item endorsed by the National Security Agency for securing classified and sensitive U.S. government information, when appropriately keyed. The term refers only to products, and not to information, key, services, or controls. They are available to U.S. government users, their contractors, and federally sponsored non-U.S. government activities subject to export restrictions in accordance with International Traffic in Arms Regulation.

U

Unacceptable Risk: A condition that, if not mitigated, could cause damage to the national security of the United States or impact on Departmental and contractor employees, the public, and/or the environment.

Unauthorized Disclosure: A communication or physical transfer to an unauthorized recipient.

Unclassified: The designation for information, a document, or material that has been determined not to be classified or that has been declassified by proper authority.

Unclassified Controlled Information: Unclassified information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552).

Unclassified Controlled Nuclear Information (UCNI): Certain unclassified Government information concerning nuclear material, weapons, and components whose dissemination is controlled under 42 U.S.C. 2168 (Section 148, as amended, of the Atomic Energy Act of 1954), DOE O 471.1A, Identification and Protection of Unclassified Controlled Nuclear Information, and DOE M 471.1-1, Identification and Protection of Unclassified Controlled Nuclear Information.

Undercover Operation: A phrase that is usually associated with the law enforcement community and which describes an operation that is so planned and executed as to conceal the identity of, or permit plausible denial by, the sponsor. Synonymous with covert operation.

V

Vulnerability: The susceptibility of information to exploitation by an adversary.

Vulnerability Analysis: A process which examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity.

Vulnerability Assessment: The results of vulnerability analysis expressed as a degree of probable exploitation by an adversary.

W **No Definition**

X **No Definition**

Y **No Definition**

Z No Definition